REMARKS

Reconsideration and allowance are respectfully requested.

Nearly all the claims stand rejected under 35 USC §103(a) as being unpatentable based on a Wireless Identity Module protocol document referred to by the Examiner as WIM in view of newly-cited Ogasawara. This rejection is respectfully traversed.

The WIM reference describes a tamper-resistant security device with a memory for storing user credentials like a security key and an AKA-module for performing AKA processing with the security key. WIM defines an interface between part of a WAP client device and the tamper-resistant security device, i.e., WIM defines an **external** interface to the security device. Page 63 of the WIM-document discloses a card (mapped to a tamper-resistant security device) incorporating a WIM-application and other applications so that these applications are protected and executed in a tamper-resistant environment. But there is no disclosure in WIM of an **internal** interface between the other applications or the WIM-application and the AKA-module. Input to and output from the WIM-application and the other applications are directed over the external interface to the tamper-resistant security device for processing by the WIM-application or other applications.

Nor does WIM disclose the claimed cooperating application, as the Examiner agrees. The Examiner relies on Ogasawara as allegedly teaching the cooperating application and contends the combination of WIM and Ogasawara teaches the claimed internal interface. Applicants respectfully disagree.

Ogasawara discloses a system for access to one or more data fields in an IC card. A user selects a field for access and provides a personal identification number corresponding to the data field. The IC card verifies the personal identification number and allows access if verification is

affirmative. The Examiner contends that Ogasawara's IC card "control program" stored in ROM is a cooperating program to permit access to a data field area in the IC.

Ogasawara's authentication is completed by verification of input personal identification number. In contrast, claim 44 recites an internal interface that allows cooperative processing between a cooperating application and the AKA module (both of which are wholly contained within the tamper security device) so that the cooperating application selectively performs enhanced security processing in conjunction with the AKA module within the tamper-resistant security device, where that enhanced security processing is part of an ongoing authentication and key agreement process being performed by the AKA module.

Once Ogasawara authenticates a personal identification number, the requested access to data field is allowed, and data may be provided to the user which ends the entire process. In contrast, claim 44 is amended to recite that "said enhanced security processing by said cooperating application includes post-processing of at least one AKA output parameter produced by the AKA module in response to the one or more AKA process commands, said post-processing including encapsulation of said at least one AKA output parameter to generate a further AKA parameter that has higher security than said at least one AKA output parameter produced in response to the one or more AKA process commands." Example support for this amendment may be found in claims 46-48, page 6, lines 9-19, page 22, line 26-page 25, line 5. The claimed cooperating application, unlike the PIN number comparison in Ogasawara, provides a post-processed response as part of an ongoing authentication process. At best, Ogasawara only processes input information with the objective to authenticate an input PIN, but in response to positive verification of the entered PIN, the requested data is simply delivered. Claim 44 also processes output information from the AKA-module. The Examiner's reference to "pre-master

secret" from WIM is not post-processing and it is not performed by the claimed cooperating

application, which the Examiner already admitted is not taught in WIM.

Nor is there a teaching in Ogasawara of post-processing an AKA output parameter

produced by the AKA module in response to an AKA process commands that includes

"encapsulation of said at least one AKA output parameter to generate a further AKA parameter

that has higher security than said at least one AKA output parameter produced in response to the

one or more AKA process commands." The Examiner's reference to sections 7.2.2.1 and 9.4.6

are not understood since the former section simply identifies a WIM-closeservice primitive "used

after using other primitives" and the latter section mentions authentication object directory files.

The claimed encapsulation needs to be done in the claimed cooperating application which the

Examiner relies on Ogasawara for rather than WIM. Moreover, it is not understood what in the

references corresponds to the (1) one or more AKA process commands, (2) AKA output

parameter, and (3) further AKA parameter that has higher security than the at least one AKA

output parameter. If claim 44 is rejected, specific identification of (1)-(3) in the prior art

reference relied on is requested.

New claims 79-82 are added directed to particular features in example embodiments from

the specification. Claim 79 recites that the one or more AKA process commands include a

random challenge and the at least one AKA output parameter includes a response to the random

challenge that matches the random challenge. Claim 80 specifies that the response is

encapsulated using a function applied to manipulate the response to produce a higher security

response. The function is a keyed function in claim 81, and claim 82 recites that the one or more

AKA process commands include multiple random challenges and the at least one AKA output

parameter includes multiple responses to the random challenges and the function is a keyed
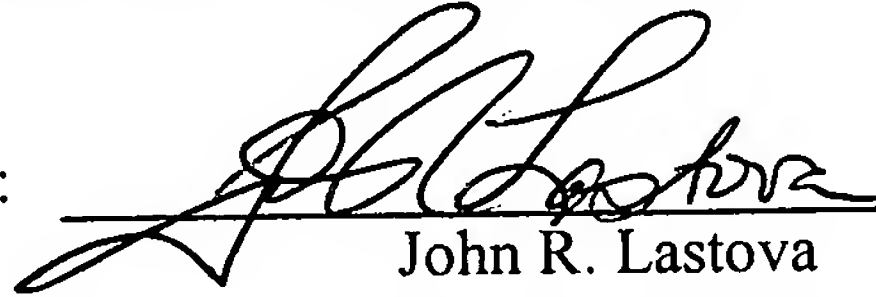
1612719

function of the multiple responses. Example support may be found on page 23, line 28-page 25, lines 5. These dependent claim features are missing from WIM and Ogasawara.

The application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000

1612719